AMENDMENTS TO THE SPECIFICATION

Page 28

Please replace the paragraph commencing at line 15 with the following amended paragraph:

At the time of T0, the key K_1 is supplied, and the encrypting process of the plaintext data M_1 is started. When the encrypting process of the plaintext data M_1 is started at the time of T0, the input of the selector 54 is switched to B after the initial value ~~IV~~ IT is once input from the input A of the selector 54. Further, at the time of X during the plaintext data M_1 is being encrypted using the key K_1, it is assumed an interrupt IT for requesting to encrypt the plaintext block data N_1 is generated. The ciphertext block data C_1 becomes to be stored in the memory 55 by the time of T1. Then, at the time of T1, the key K_2 is supplied to the encrypting module 51 due to the generation of the interrupt IT. Further, the selector 54 sets the input to A at the time of T1. The switch 57 is connected to F at the time of T1. After the time of T1, the plaintext block data N_1 is encrypted using the key K_2, and the ciphertext block data D_1 is output. At the time of Y, it is assumed the encryption of the plaintext block data N_1 is finished, and the interrupt IT is resolved. Due to the resolution of the interrupt IT, at the time of T2, the key K_1 is supplied to the encrypting module 51, the input of the selector 54 is switched to C, and the switch 57 is connected to E. By switching the selector 54 to C, the ciphertext block data C_1 stored in the memory 55 is input for encrypting the plaintext block data M_2, the plaintext block data M_2 is encrypted by the encrypting module using the key K_1, and the ciphertext block data C_2 is output. Before the time of T3, the input of the selector 54 is switched to B. In case of encrypting the plaintext block data M_3, the ciphertext block data C_2 is fed back from a feedback line 65 of a feedback loop and input, the plaintext block data M_3 is encrypted by the encrypting module using the key K_1, and the ciphertext block data C_3 is output.